



Bildquelle: Tim Grams, online unter
<https://derbloggendebahner.de/downloads/>



Digital Rail

Auftaktveranstaltung

23. April 2025

Agenda

- Einführung und Motivation
- Vorstellung der Fachgebiete
- Lehrveranstaltung
 - Ablauf
 - Projektvorstellung
- Nächste Schritte

Digital Rail

Domänenwissen

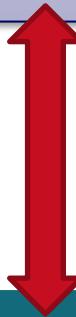
aus 3 Dimensionen



Zulassung (EN 50126 ff., CSM)

Sicherheitsnachweis

Nachweis (= praktischer Beweis) und Gutachten, dass das System (Gesamtsystem) immer einen sicheren Zustand annimmt



Wie kann moderne IT im Rahmen bestehender Gesetze und Vorgaben zugelassen und in Betrieb genommen werden?
Wie kann IT bei den aktuellen Herausforderungen im Bahnwesen helfen?
....

Digitale LST

Bahnbetrieb: Züge fahren

Produktionsprozesse des Bahnbetriebes (Fahrdienstvorschrift, Signalbuch)

Geschwindigkeiten, Längen/Abstände, Fahrstraßen, Fahrerlaubnisse

BTSF

(Betrieblich-Technische Systemfunktionen; FRS & SRS = Functional & System Requirement Specification)

Informatik (Softwaretechnik)

Modellgetriebene Entwicklung, V-Modell, Agil
Simulation, Verifikation, Komponenten, Test, Fehlerinjektion, Kontinuierliche Integration, DevOps

Co-Simulation, IoT-Labor, Feldtest Reallabor / Living Lab

Nichtfunktionale Systemeigenschaften: Echtzeit, Fehlertoleranz, Sicherheit

- Zusammenarbeit
 - bevorzugt domänenübergreifende/interdisziplinär
- Lehrvideos aus den verschiedenen Domänen
- Sprechstunden
- Gastvorlesungen
- Exkursionen
- Projektwoche (Sommerschule, *Summer School*)
- Projektarbeit in kleinen (interdisziplinären) Gruppen
- Bewertung nach Maßgabe der Heimatuniversität

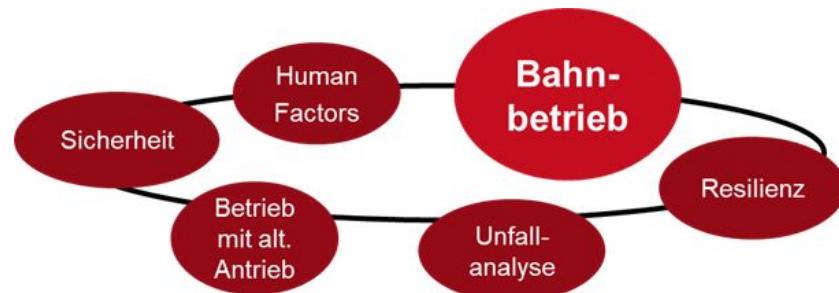


Vorstellung der Fachgebiete

Ziel in Lehre und Forschung:

Betrachtung des Schienenverkehrs als Gesamtsystem

www.railways.tu-berlin.de



Ausstattung

- Eisenbahn-Betriebs- und Experimentierfeld
 - Echte Stellwerke bedienen
- Fahrsimulatoren



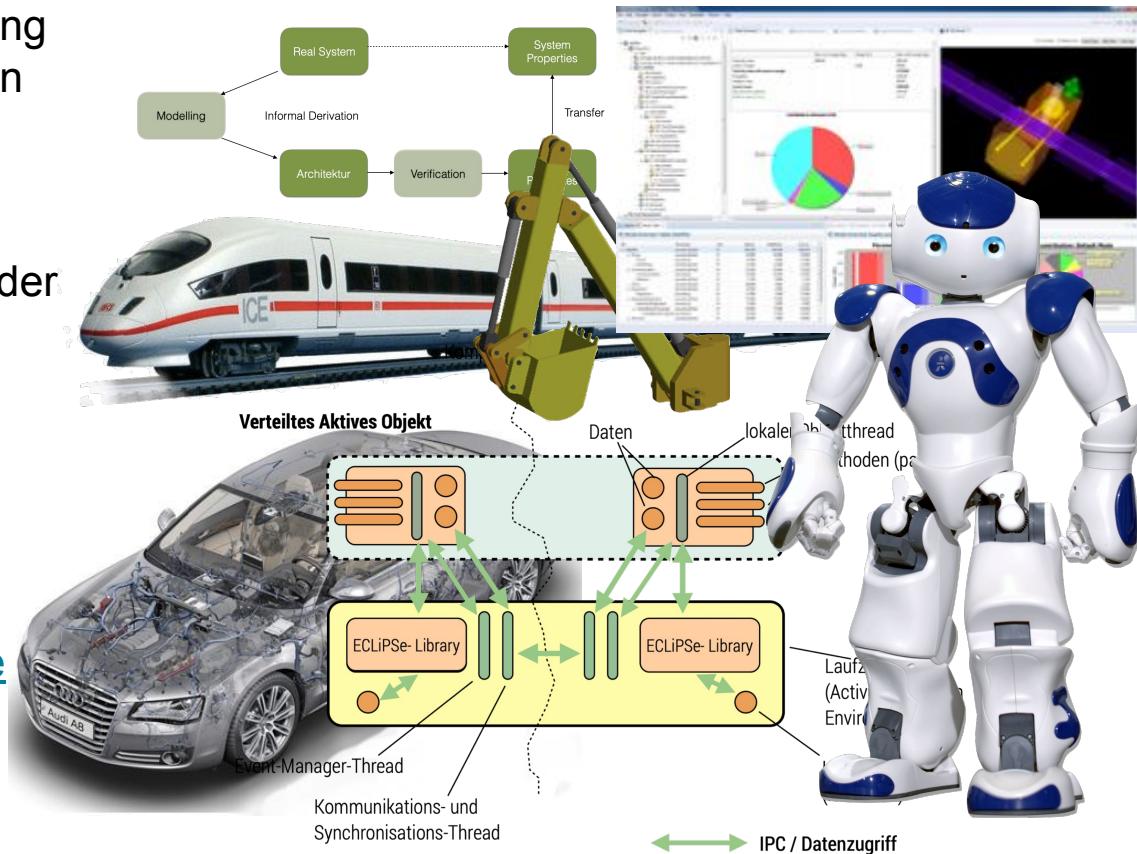
Forschungsschwerpunkte:

- Modellierung und Gewährleistung meta-funktionaler Eigenschaften
- Moderne Laufzeitsysteme für dynamische Anwendungen

Anwendung vorwiegend im Bereich der mobiler Systeme, insbesondere
Transportation Systeme

- Automobile
- Bahn
- Raumfahrt
- Nutzfahrzeuge

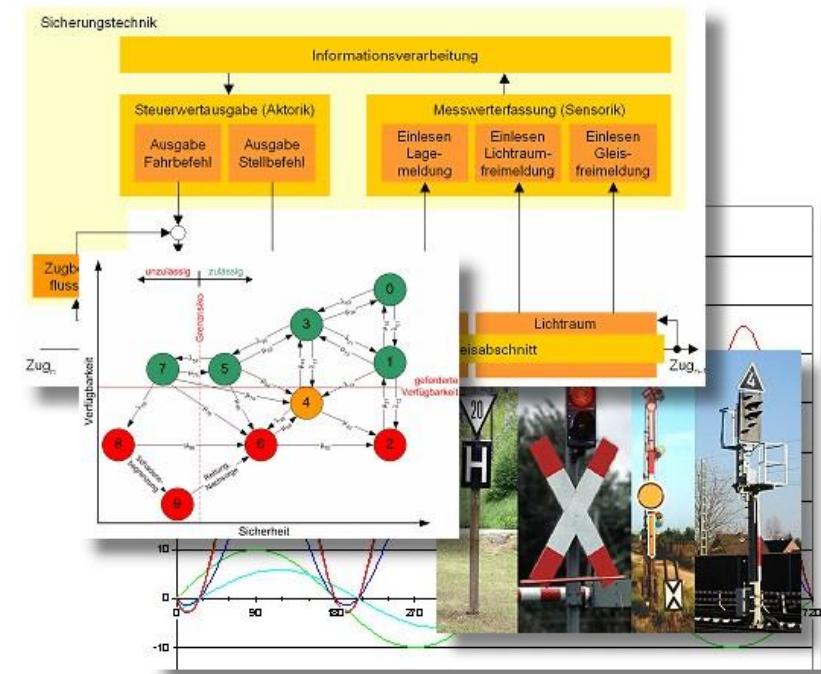
<https://osg.informatik.tu-chemnitz.de>



Wissenschaftlicher Gegenstand:
Steuerung und Sicherung
spurgeführter Verkehrssysteme
Dafür werden folgende
wissenschaftlichen Disziplinen vereint:

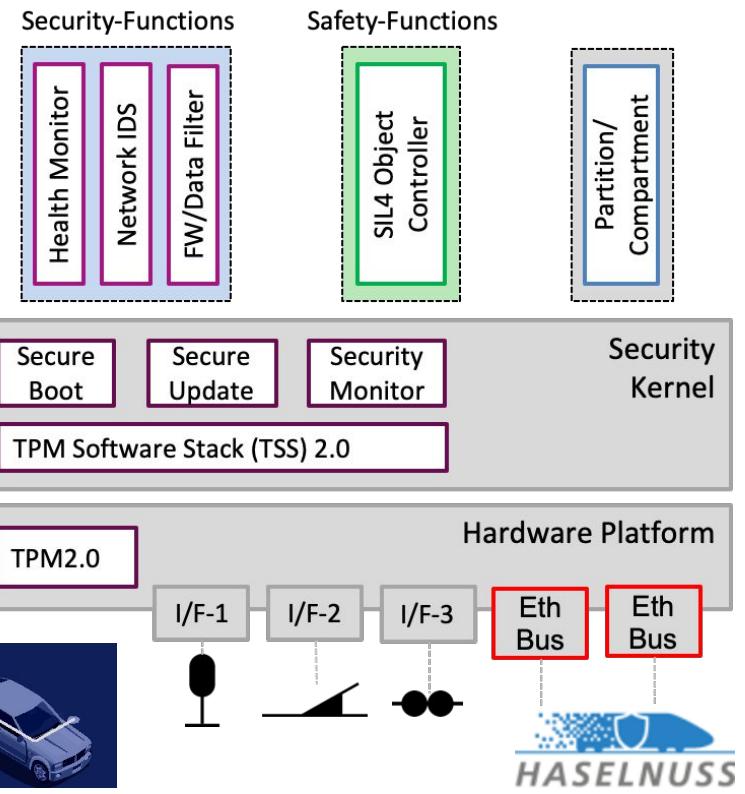
- Sicherheitswissenschaft
- Eisenbahnbetriebswissenschaft
- Automatisierungstechnik

<https://tud.de/vst>



Forschungsschwerpunkte:

- IT-Sicherheit, Hardware-nahe Sicherheit
- Sichere kritische Infrastrukturen
- Digitalisierung im Schienenverkehr





“Middleware für vorhersagbares Systemverhalten”

- Paradigmen, Entwurfsmuster, Implementierungsstrategien
- Echtzeit (*real-time*), Verlässlichkeit, IT-Sicherheit



Betriebssysteme

- Neue Konzepte für neue Hardwareparadigmen (NUMA, GPU, FPGA, POWER)
- Programmiermodelle für Beschleuniger und lokal verteilte Systeme

weit verteilte Systeme – Grid, Cloud, IoT

- vorhersagbares Verhalten in heterogenen verteilten Systemen
- dienstorientierte Cloud-Umgebungen



eingebettete Systeme

- analytische Redundanz, Reparatur im Betrieb, dynamische (Re)Konfiguration

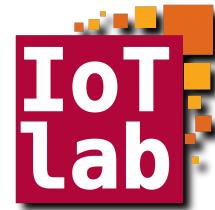
Kontakte (osm.hpi.de/people)

- Arne Boockmeyer, Dirk Friedenberger, Lukas Pirl, Robert Schmid, Prof. Andreas Polze

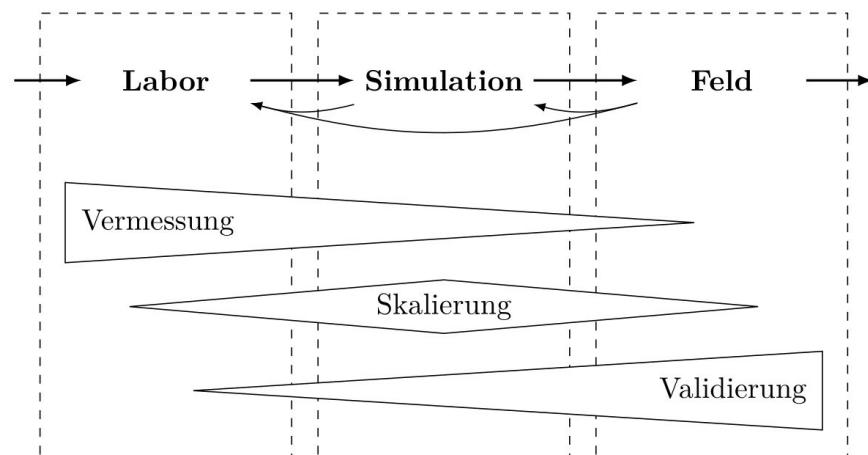


Betriebssysteme & Middleware (HPI)

Labor für IoT



- Prototypen erstellen & testen
- Kopplung von Domänen
- modellgetriebene und modellunterstützte Ansätze
- Automatisierung & Alternativen zu spezialisierten Testumgebungen
- Schwerpunkt Interoperabilität und Verlässlichkeit
- hybride, co-simulierte und verteilte Experimente



Digitalisierung Entwicklung, Zulassung, Abnahme, Betrieb

- Generierung von Software aus Spezifikationen
- Automatisierte, verteilte Tests

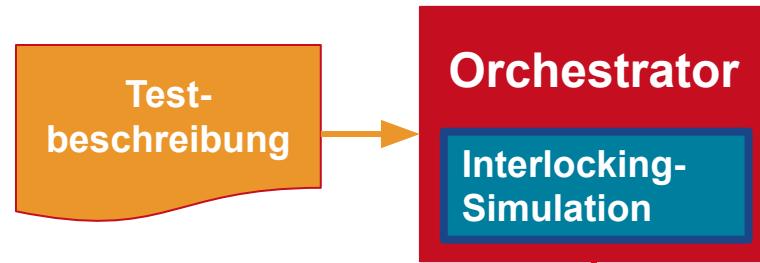
Neutraler Grund zw. Herstellern und Betreibern

- Verteilte Laborumgebung
- Interoperabilitätstests, Co-Simulation

Wechselnde Hardware, teils Prototypen

- Achszähler (Frauscher, Siemens)
- *Object Controller* (Thales)
- Weichenantriebe (voestalpine, Pintsch)
- Lichtsignal (Thales)





Laborknoten

RaSTA-Bridge



HPI IoT-Lab,
Potsdam

Laborknoten

RaSTA-Bridge



Brunel,
Hildesheim

Laborknoten

RaSTA-Bridge



Digital Rail Lab,
Scheibenberg

Laborknoten

RaSTA-Bridge



DLR,
Braunschweig

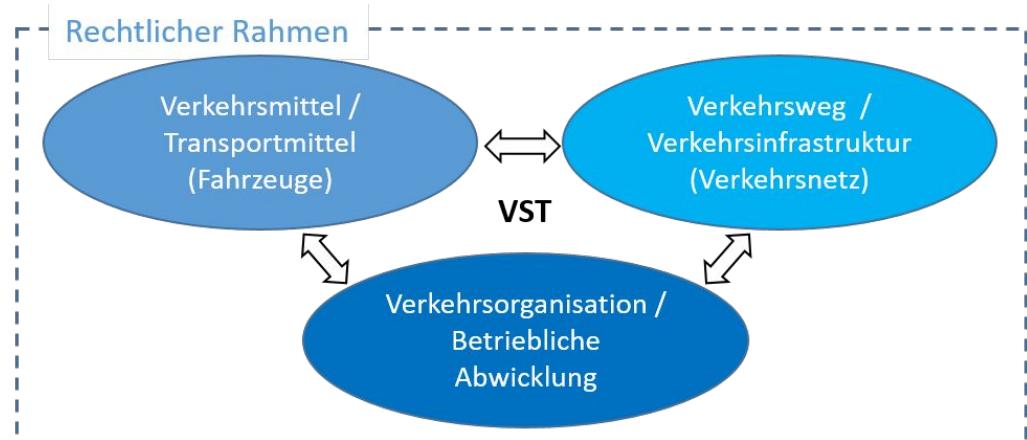
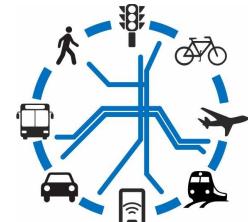
Ziel in Lehre und Forschung:

- grundlegendes Gesamtverständnis des Systems Verkehr aus Sicht der Nutzer und Betreiber von Fahrzeugen und Betriebszentralen

Themengebiete der Professur:

- Verkehrstelematik, IT im Verkehr und Datenmanagement im Personenverkehr
- Leit- und Sicherungstechnik
- Fahrerassistenzsysteme

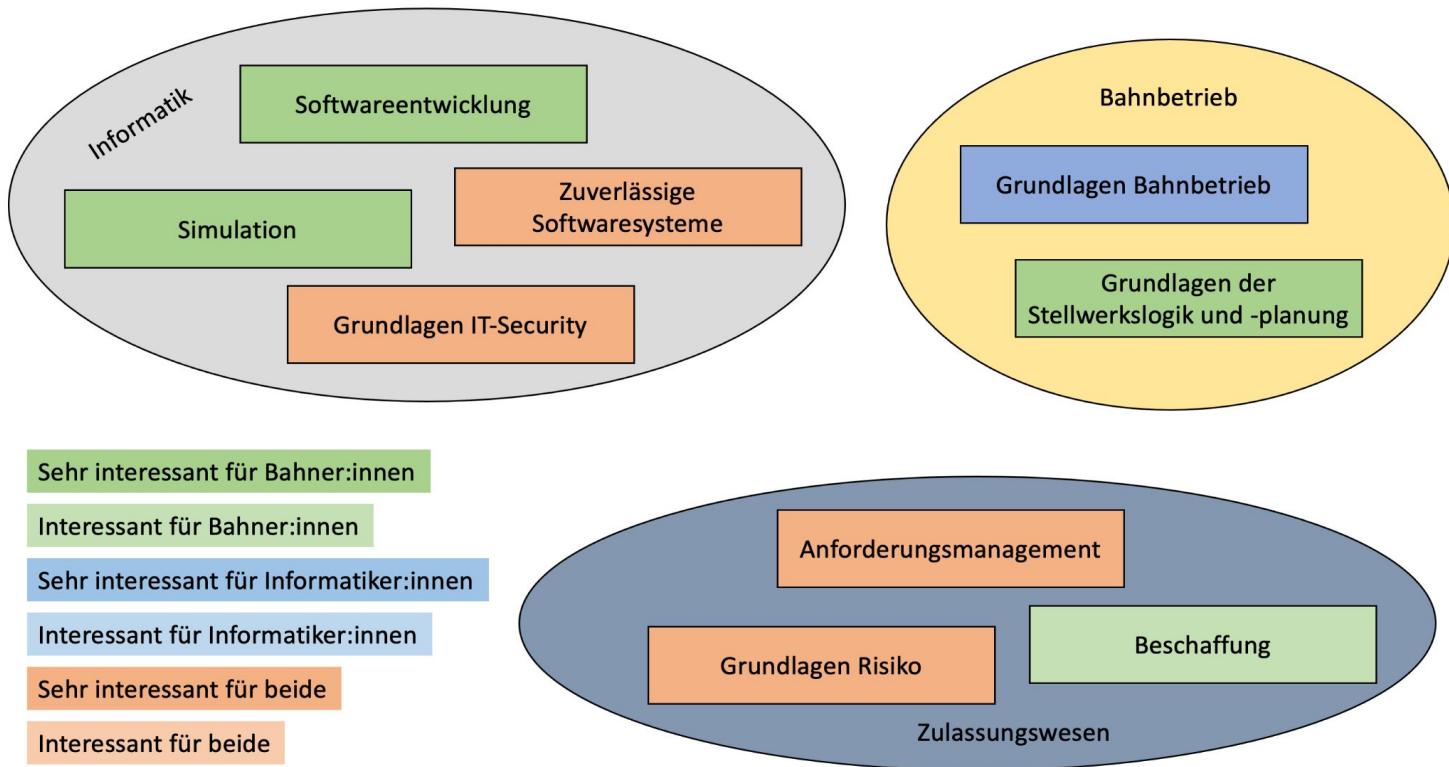
<https://www.th-wildau.de/vst/>



Die Lehrveranstaltung

- Zusammenarbeit
 - bevorzugt domänenübergreifende/interdisziplinär
- Lehrvideos aus den verschiedenen Domänen
- Sprechstunden
- Gastvorlesungen
- Exkursionen
- Projektwoche (Sommerschule, *Summer School*)
- Projektarbeit in kleinen (interdisziplinären) Gruppen
- Bewertung nach Maßgabe der Heimatuniversität

Zu hörende Lehrvideos: osm.hpi.de/drss/2025/curriculum (demnächst)



Die genaue Auswahl der Videos erfolgt in Abstimmung mit der Heimat-Uni und dem Projekt

- Vorlesungsplanung: osm.hpi.de/drss/2025/curriculum (demnächst)
- Gastvorträge mittwochs ab 11 Uhr, Videokonferenz
 - 11. od. 18.06: Dr. Kristian Weiß (Siemens Mobility): *Objekterkennung*
- Verkehrswissenschaftliches Kolloquium
 - ein Mittwoch im Monat, 15 Uhr (auch **heute**)
- Bahnsystemkolloquium
 - ausgewählte Donnerstage, 14:50 – 16:20 Uhr
- Eisenbahnwesen-Seminar
 - Montags, 18:15 – 19:45 Uhr
- Exkursionen
 - Mittwoch, 02.07.: Eisenbahn-Betriebs- und Experimentierfeld (EBuEf)
 - Termin ausstehend, BahnTechnologie Campus (BTC) Havelland

- TU Berlin
 - 6 ECTS: 50 % MC-Test zu Inhalten ausgewählter Lehrvideos, 50 % Projekt
- HPI
 - 6 ECTS: 50 % Prüfung zu Inhalten ausgewählter Lehrvideos, 50 % Projekt
- TH Wildau
 - 5-6 ECTS je nach Studiengang:
50 % MC-Test zu Inhalten ausgewählter Lehrvideos, 50 % Projekt
- TU Chemnitz
 - 5 ECTS: für die Projektarbeit (Projektbericht + Abschlusspräsentation)
 - 3 ECTS: mündliche Prüfung zu Inhalten ausgewählter Screencasts
- TU Dresden
 - 5 ECTS: Note: Bewertung der Projektarbeit und Präsentation
- Uni Passau
 - 12 ECTS:
Bewertung der Projektarbeit und Präsentation (+ interne Präsentationen)

bitte allen externen Vorträgen unseres Curriculums und zwei weiteren Vorträgen beiwohnen

- Partner bieten ein oder mehrere Projekte an
- Beginn, Ablauf, Umfang, Anforderungen sind mit der jeweiligen verantwortlichen Einrichtung zu klären
 - #1: Automatisches Rangieren: Anforderungen und Implementierung (TU Berlin)
 - #2: Von der Planung, ins Labor, bis zu Tests – durchgängig digital (HPI, TU Dresden)
 - #3: Securing Railway Intrusion Detection Environments (Uni Passau, INCYDE GmbH)
 - #4: Sicherheitsanalyse EULYNX (HTWD, TU Chemnitz, HPI, TH Wildau)
 - #5: IT-Sicherheitsanalyse von GSM-R (HTWD, HPI)

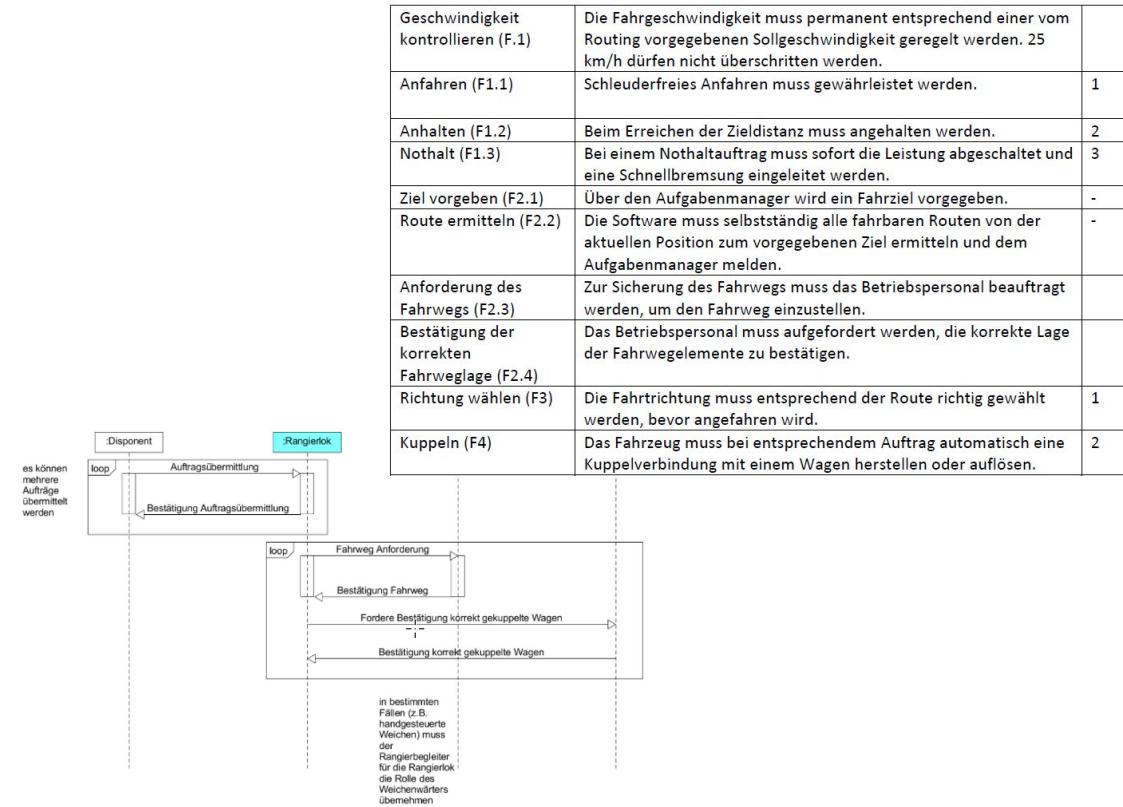
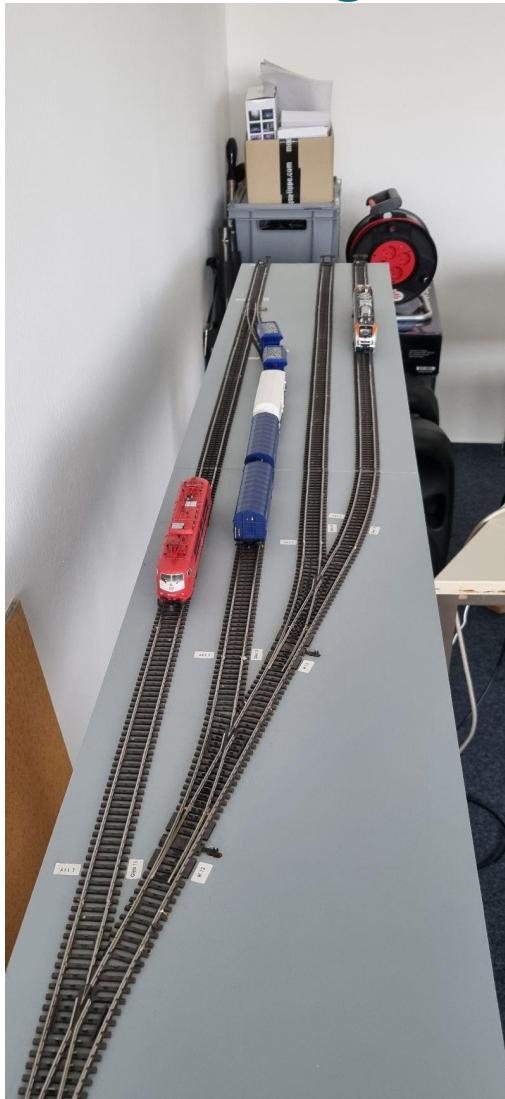
Automatisches Rangieren: Anforderungen und Implementierung (I)



- Das BBI-Projekt wird sich mit dem Thema Rangierroboter auseinandersetzen.
- Rangieren ist sehr personalintensiv → hohe Kosten für EWV
- Im ersten Teil des Projekts wird das Thema Anforderungsableitung inkl. Risikobetrachtung behandelt.
- Im zweiten Teil des Projekts werden Sie selbst ein IT System designen und zum Abschluss einen Modellbahn-Rangierroboter steuern. IT-Kenntnisse werden nicht vorausgesetzt, sondern im Rahmen der Vorlesung vermittelt.
- Arbeit in Kleingruppen
- Präsenz und Online-Termine
- Auftakt für das bbi-Projekt am 30.4. 12:30 Uhr (SG12 204)

Automatisches Rangieren

Anforderungen und Implementierung (II)



Consequence	Frequency	Possibility	Probability	Risikominderung	SIL
C3	F1	X	W1	d	2

Von der Planung, ins Labor, bis zu Tests – durchgängig digital

Arbeitspaket 1: verstehen & reproduzieren

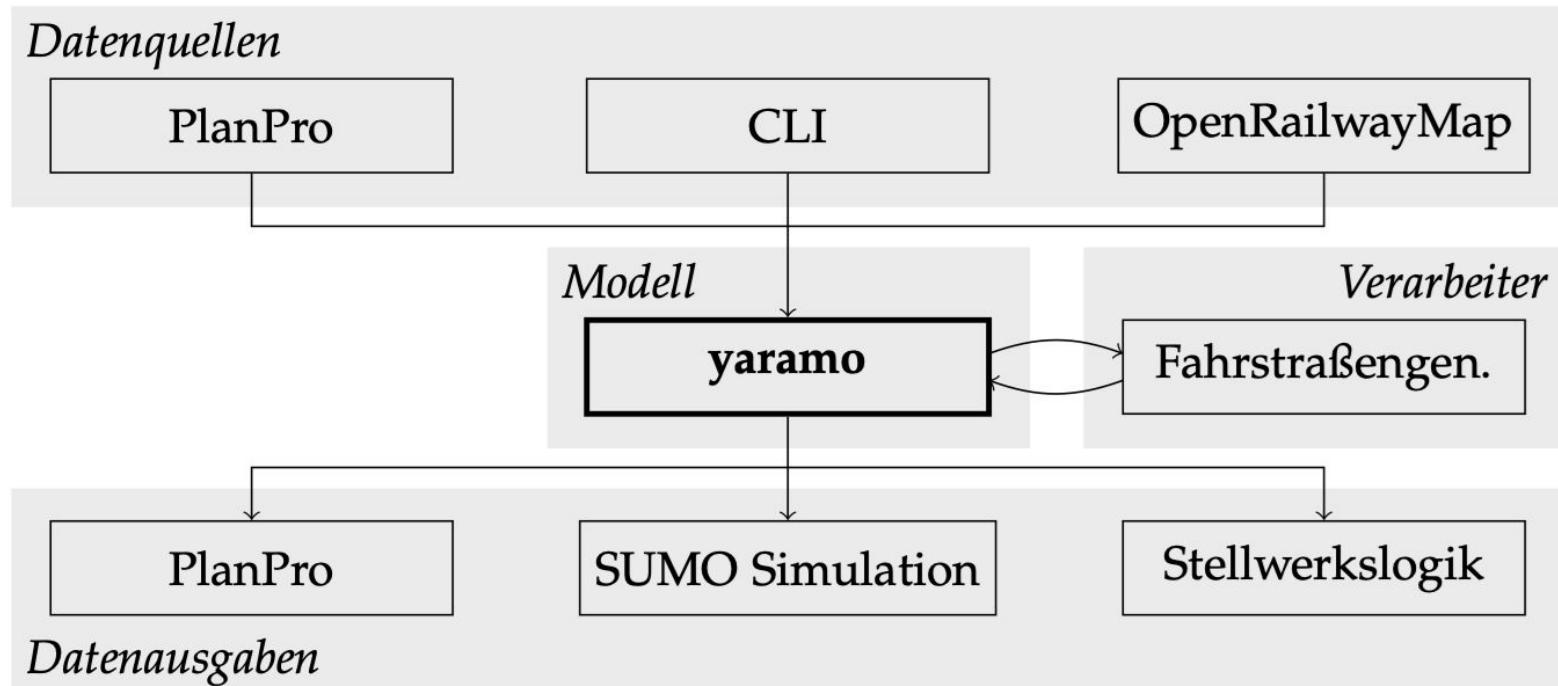
- von digitalen Planungsdaten zur Ansteuerung von Feldelementen
- Planungsdaten auslesen
- Stellwerkslogik parametrisieren
- Feldelemente über EULYNX ansteuern

Arbeitspaket 2: entwerfen & produzieren

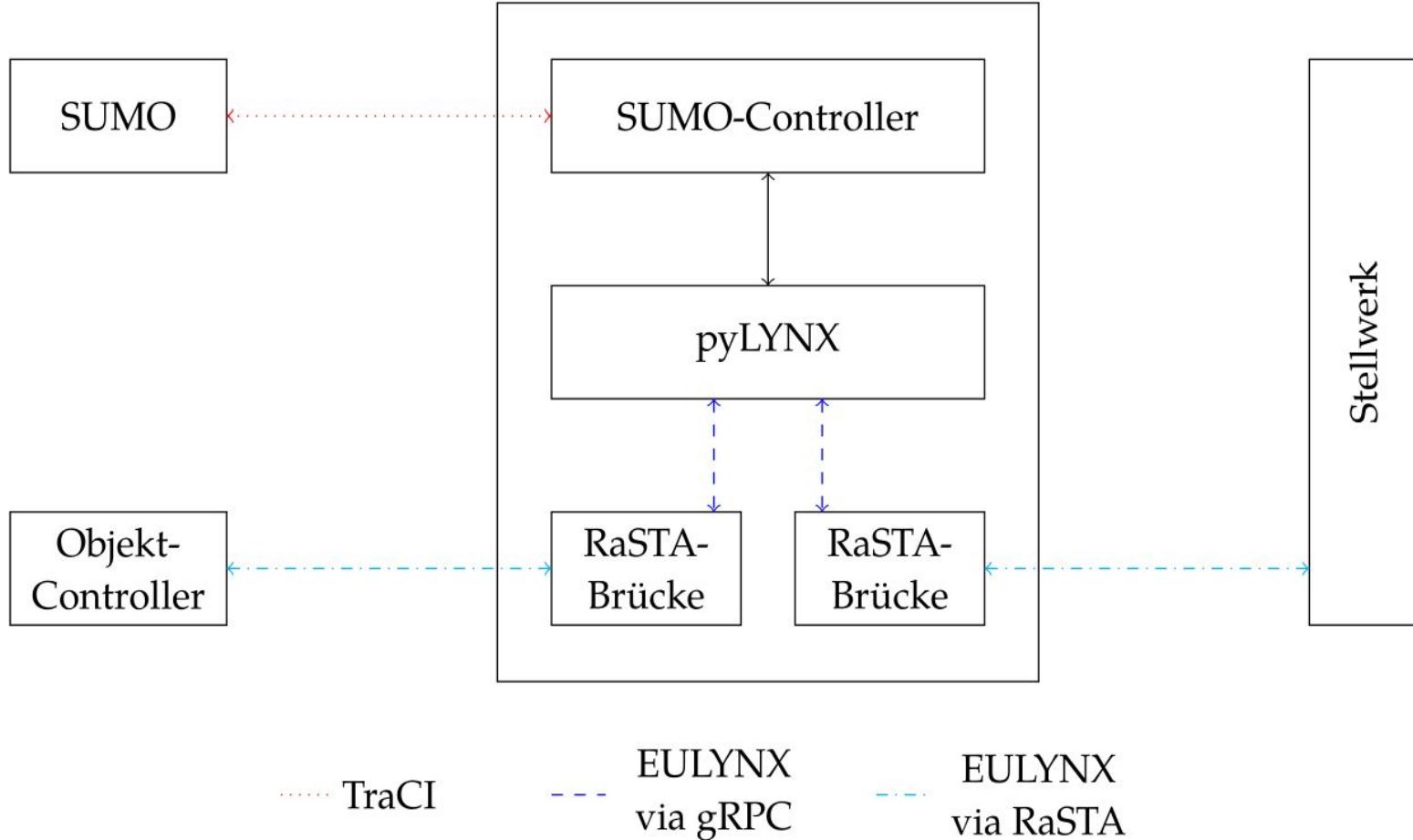
- fachliche Testabdeckungskriterien entwickeln
- Bediensoftware für Lichtsignal und Zusatzanzeiger erstellen
- parametrisierbaren Testtreiber entwerfen
- Tests aus digitalen Planungsdaten ableiten
- Tests evaluieren

Ansprechpartner: [Arne](#), [Lukas](#), [Robert](#), [Richard Kahl](#)

Von der Planung, ins Labor, bis zu Tests – durchgängig digital

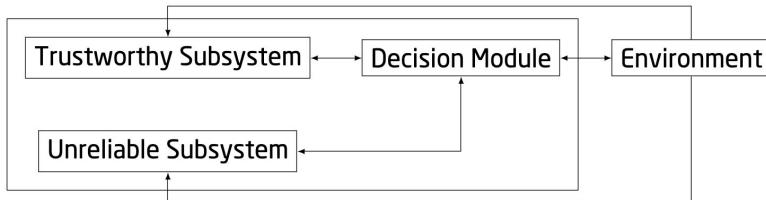


Von der Planung, ins Labor, bis zu Tests – durchgängig digital



Simplex-Architektur: Softwareupdates für Bahnkomponenten

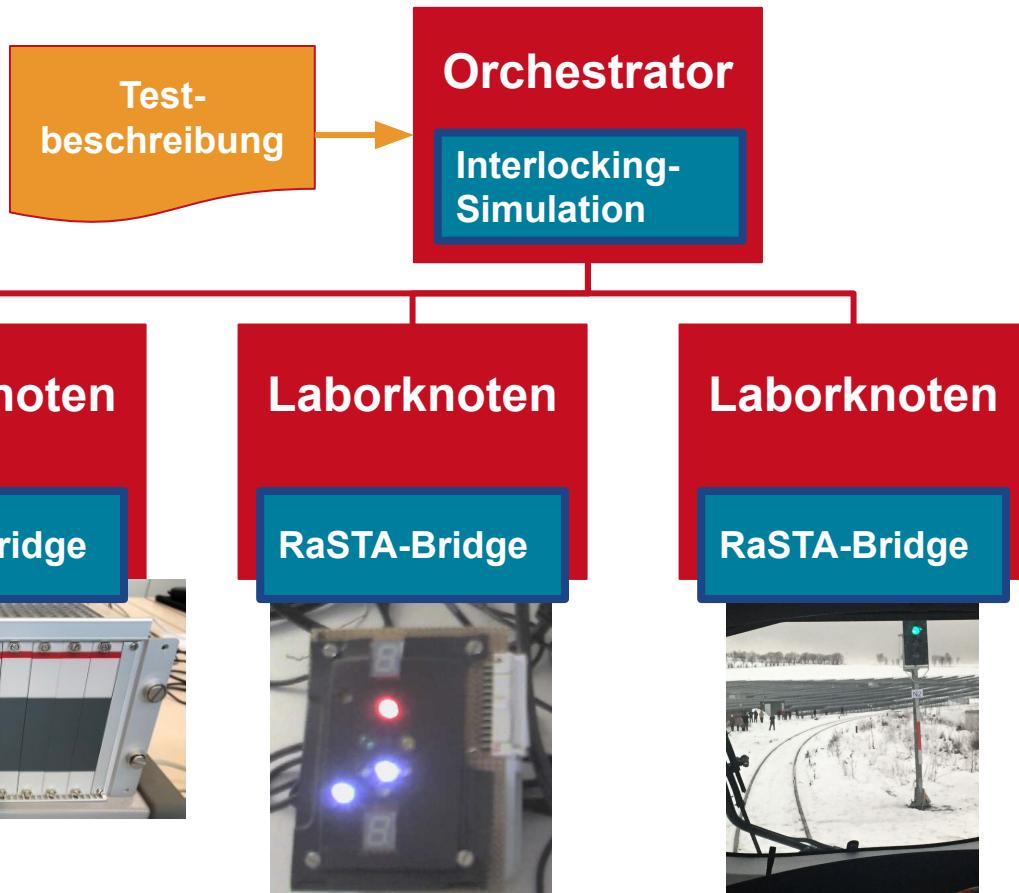
- Funktionale Sicherheit in den Softwarekomponenten muss durchgängig gewährleistet werden
- Funktionsupdates im nicht-sicherheitskritischen Teil sind wünschenswert
- Lösung: Überwachungskomponente, die die Verlässlichkeit des sicherheitskritischen Systemteils durchgehend überwacht



Simplex-Architektur [Sha 01]

Projektidee: Achszählsystem (z.B. Siemens, einer selbstprogrammierten Simplex-Überwa

zu überarbeiten



HPI IoT-Lab,
Potsdam

Brunel,
Hildesheim

Digital Rail Lab,
Scheibenberg

Securing Railway Intrusion Detection Environments

Motivation

- Wachsende Bedrohung durch Digitalisierung der Bahn
- Safety-kritische Systeme müssen vertrauenswürdig bleiben
- Wie erkennen wir Angriffe und Manipulationen?

Intrusion Detection Systeme (IDS)

- System zur Erkennung von Angriffen, Anomalien oder unerwünschten Aktivitäten
- Typen: Host-basiert und Netzwerk-basiert
- Erkennungsverfahren: Signatur-basiert (Erkennung von Mustern), Anomalie-basiert (Erkennung durch Abweichung vom Normalverhalten)

Security Information and Event Management (SIEM)

- Zentrale Sammlung, Korrelation und Auswertung sicherheitsrelevanter Ereignisse
- Ermöglicht Überblick, Analyse, Alarmierung
- Aufbereitung der Daten des IDS

Problemstellungen

- Wie lassen sich Sicherheitsdaten verständlich darstellen, korrelieren und bewerten?
- Wie erkennt man potentielle Angriffe oder Anomalien, bevor Schaden entsteht?
- Wie kann die Integrität des IDS sichergestellt werden?
- Wie kann sichergestellt werden, dass kritische Komponenten eines Systems während der Laufzeit nicht manipuliert wurden?

Securing Railway Intrusion Detection Environments

(1) Aufbau eines Security Information and Event Management Systems

- Sammlung, Korrelation, und Analyse von Daten
- Erstellung von Dashboards zur Visualisierung relevanter Daten/Ereignisse

(2) Entwicklung einer Runtime Integrity Überwachung

- Integritätsüberwachung von einzelnen Dateien/Prozesse bis hin zu Ausführungsumgebungen
- Einbindung der Daten in SIEM/Dashboards

(3) Formalisierte Beschreibung IDS Alarme

- Wie können Vertrauensketten formal beschrieben werden?

(4) Vertrauensketten beschreiben

- Vertrauensketten für: Data at Rest, Data in Transit, Data in Operation

Securing Railway Intrusion Detection Environments

Euer Beitrag:

- Gutes Teamwork, Spaß am gemeinsamen “Tüfteln”
- Selbstständiges Arbeiten
- Programmiergrundkenntnisse

Euer Benefit:

- Tiefe Einblicke zu Security in Kritischen Infrastrukturen
- Umgang mit IDS-Systemen, SIEM, und Dashboards
- Hacking = Fun

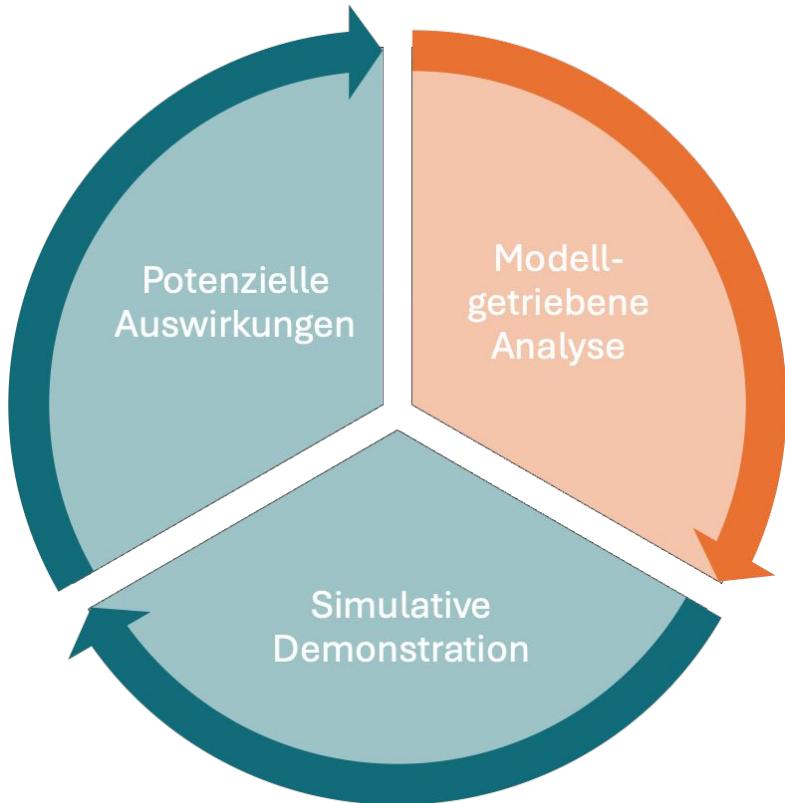
Betreuung:

- Simon Unger (Uni Passau)
- Dominik Spychalski (INCYDE GmbH)

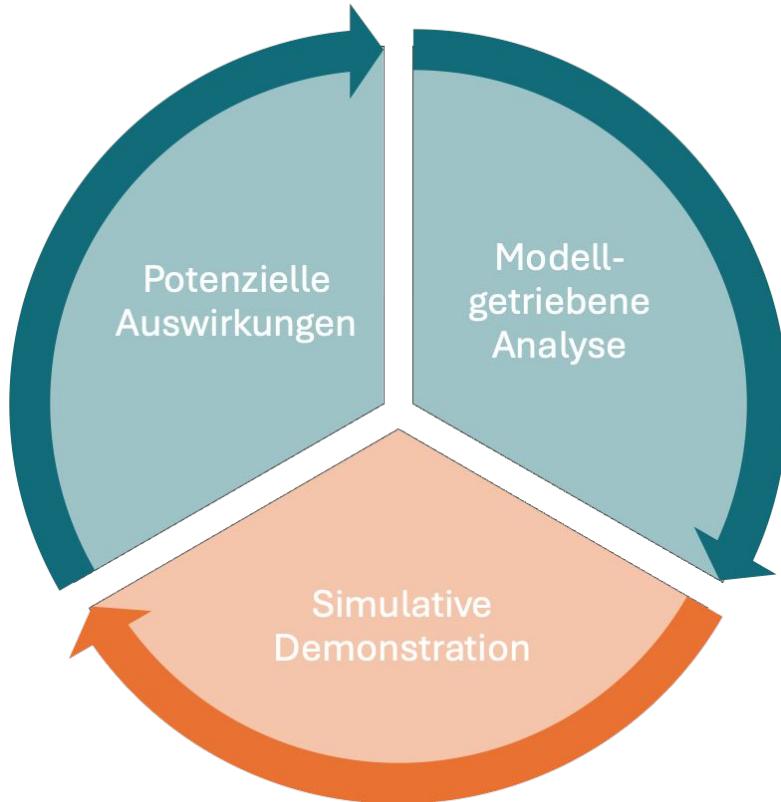
- Testen und Auditieren ...
 - können “nur” Fehler aufzeigen, nicht aber ihre Abwesenheit (Korrektheit des Systems)
 - funktionieren weitgehend nur für eine konkrete Implementation

→ Reichen “Testen und Auditieren” für die Sicherheit im Bahnbereich aus?

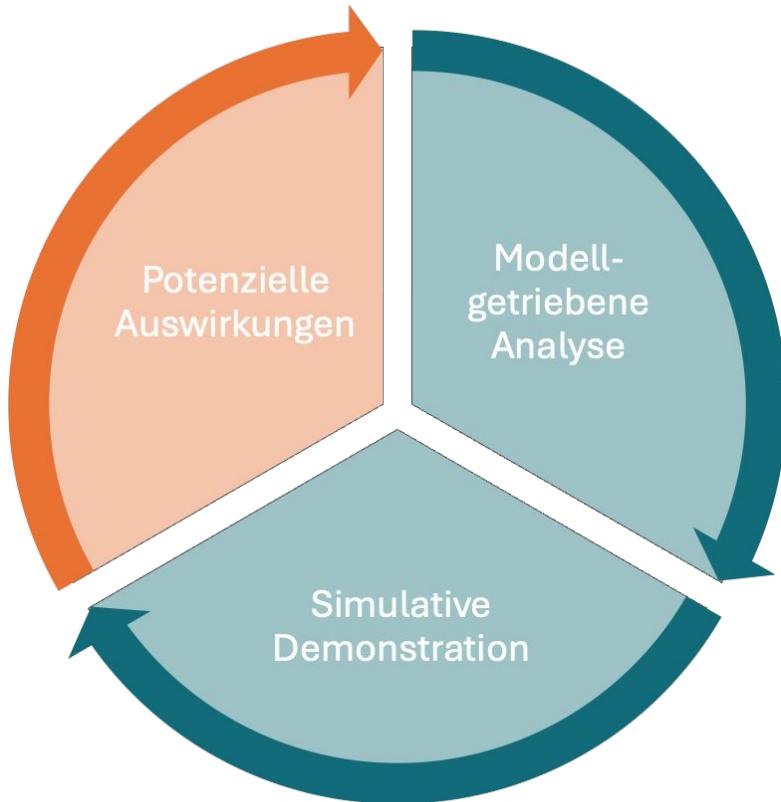
→ Welche Alternativen gibt es?
- Modelle
 - Verallgemeinern von konkreten Implementationen auf Aussagen über Konzepte
 - können bereits auf Spezifikationsebene Fehler finden



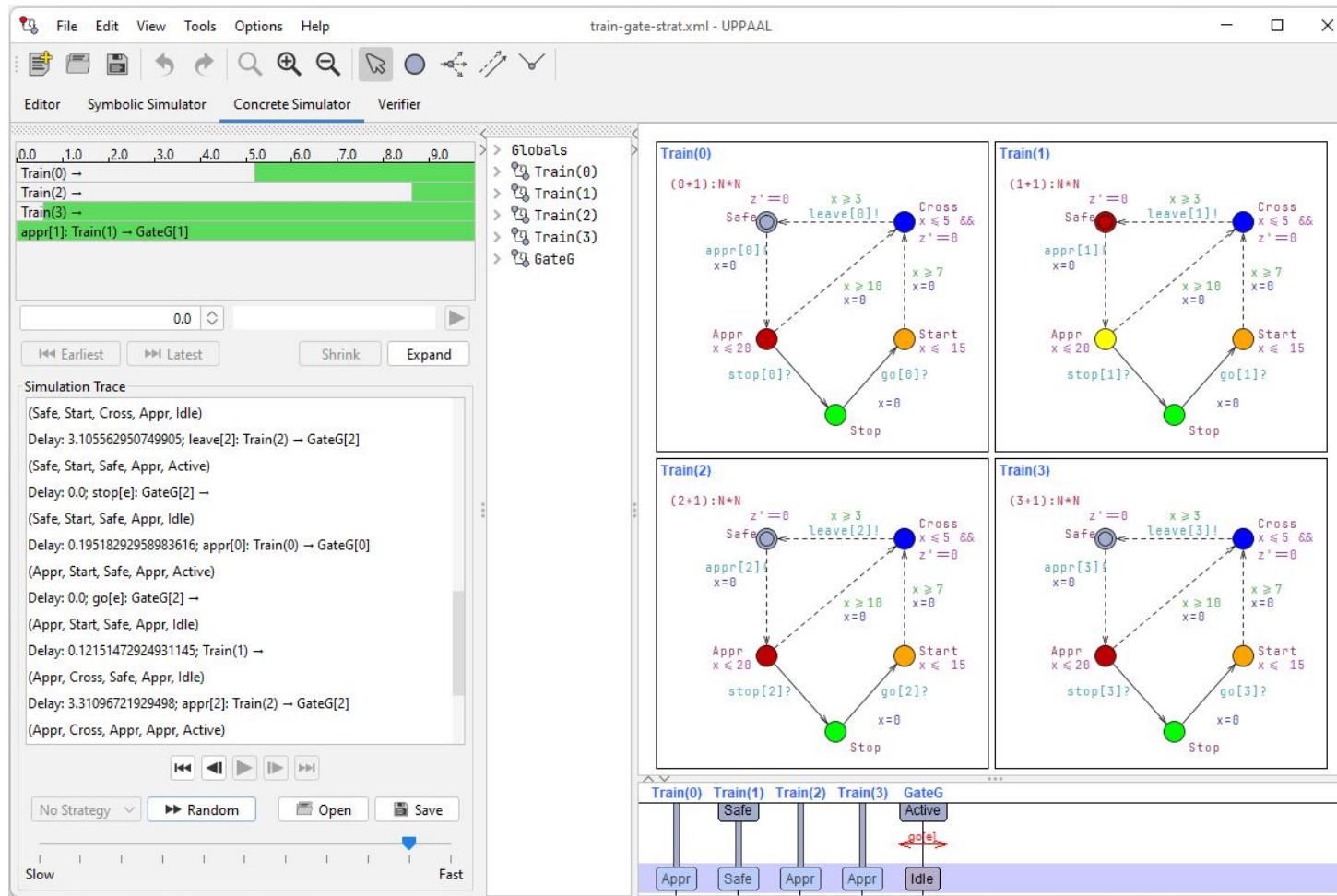
- Modellierung von RaSTA und SCI-P in Tamarin oder ProVerif
- Analyse der Modelle auf verschiedene Angriffsmöglichkeiten, z.B.
 - Replay-Attacken
 - Man-in-the-Middle
 - Denial-of-Service



- Analyseergebnisse schön und gut...
- Wir wollen zeigen, dass die Ergebnisse auf den Modellen auch mit der Realität übereinstimmen
- Simulation der entdeckten Angriffe in einer virtuellen Umgebung



- Technische Probleme sind die eine Seite...
- Was bedeuten diese für den Bahnbetrieb?
- Kann es zu Situationen kommen, die die Safety gefährden?
- Wie lange kann eine Reparatur dauern?



Ziele

- Modellgetriebene Analyse von RaSTA und SCI-P
- Simulative Demonstration gefundener Schwachstellen
- Analyse möglicher Auswirkungen auf den bahnbetrieblichen Ablauf

Euer Beitrag:

- hochschulübergreifende Teamarbeit
- Know-How in den Bereichen Security, Implementation und Bahnbetrieb

Euer Benefit:

- Schulung in modellgetriebener Security-Analyse
- Neue Perspektiven durch fachübergreifende Zusammenarbeit

Euer Beitrag:

- Lust auf neue Perspektiven
- Spaß an der fachübergreifenden Zusammenarbeit (Bahnsystem/-wissen & Informatik)
- Spaß an der Zusammenarbeit im Team mit Studierenden anderer Hochschulen/Unis, Fachrichtungen, Semester, ...
- Spaß am Denken in abstrakten Modellen und auf bisher vielleicht ungewohnten Wegen

Euer Benefit:

- Schulung in Modellierung und formalem Denken
- Kennenlernen eines State-of-the-Art Tools (Uppaal, u.a. bei Airbus im Einsatz)
- Freude an der Arbeit im Team, beim Austausch von (neuen) Ideen und Sichtweisen

Nachvollziehbare Anforderungen für formale Spezifikationen in der LST

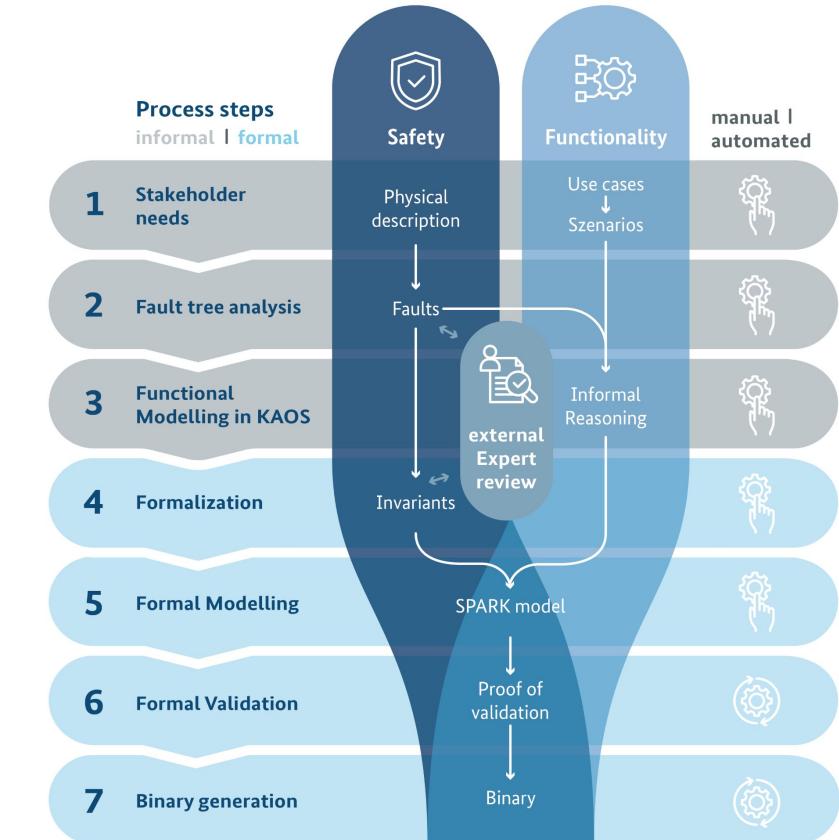
Motivation:

- Interpretationsspielräume in Spezifikationen führen zu Ineffizienzen und Interoperabilitätsproblemen
-> Ansatz: **formale Methoden statt natürlicher Sprache**
- Komplexe Regelwerke haben keinen Mechanismus zum Entdecken von Redundanzen oder Obsoleszenzen
-> Ansatz: **Traceability im Anforderungsmanagement**

Ziel:

- Entwicklung kleinstes Set an Regeln für sichere ETCS Fahrzeug-Komponente
- Formale Spezifikation einer ETCS Fahrzeug-Komponente in AdaCore SPARK

1. Erarbeitung der Stakeholder-Anforderungen
2. Fehlerbaum-Analyse und funktionale Analyse im integrierten Tooling (*Eisenbahn-Schwerpunkt*)
3. Formalisierung in SPARK (*Informatik-Schwerpunkt*)
4. Demonstration



REQ-2 Die dem Zug zugewiesenen Positionen sind ebenfalls einem anderen Zug zugewiesen

Die Mengen der jedem Zug zugewiesenen Positionen müssen disjunkt sein

$$\forall t_A, t_B \in \text{Trains}: t_A \neq t_B \Rightarrow \text{TrainAreas}(t_A) \cap \text{TrainAreas}(t_B) = \emptyset$$

SPARK

```
function EnsureDisjointAreas return Boolean is
  (for all Train1 in RegisteredTrains'Range =>
    (for all Train2 in RegisteredTrains'Range =>
      (if RegisteredTrains (Train1) /= RegisteredTrains (Train2) then
        (for all Loc1 in TrainAreas (Train1)'Range =>
          (for all Loc2 in TrainAreas (Train2)'Range =>
            TrainAreas (Train1) (Loc1) /= TrainAreas (Train2) (Loc2)
          )
        )
      )
    )
  )
)
```

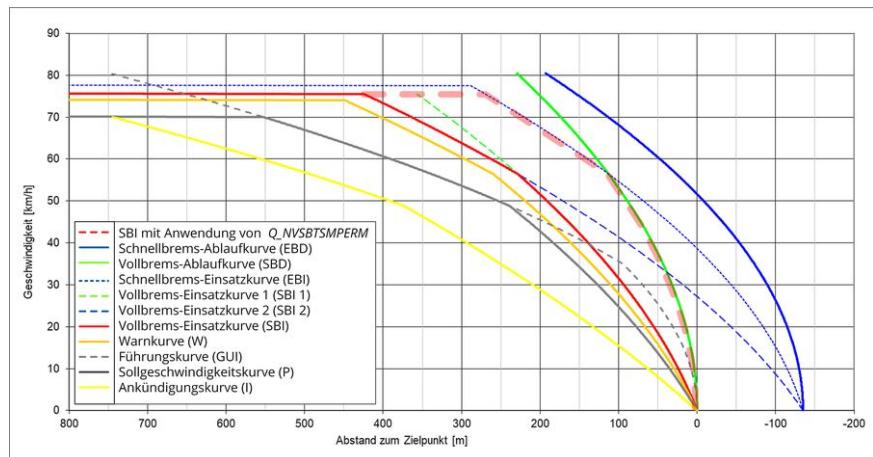
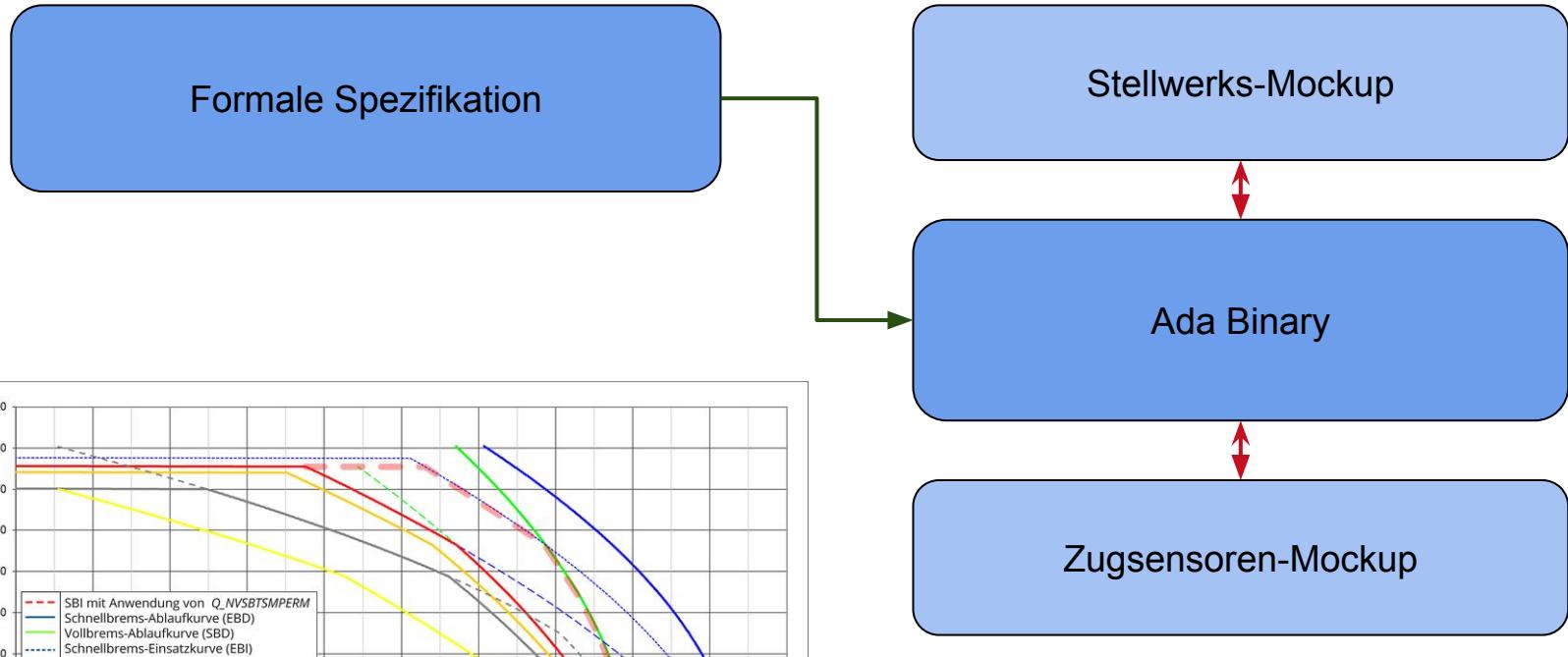
APS autorisiert Fahrzeugbewegung zu Position, die von Fahrzeug belegt wird

Autorisierte Position ist nicht Teil der dem Zug zugewiesenen Positionen

Die dem Zug zugewiesenen Positionen sind ebenfalls einem anderen Zug zugewiesen

REQ-1

REQ-2



Euer Beitrag:

- Lust auf neue Ansätze
- Validierung von neuer Methode des Anforderungsmanagements
- Beitrag zur angewandten Forschung

Euer Benefit:

- Kennenlernen von formalen Methoden in der Eisenbahnwelt
-> zukunftssicheres Know-how!
- Arbeit im interdisziplinären Team
- Anschauliches Endergebnis des Projektes

- #1: Automatisches Rangieren: Anforderungen und Implementierung
timo.ramsdorf@tu-berlin.de
- #2: Von der Planung, ins Labor, bis zu Tests – durchgängig digital
arne.boockmeyer@hpi.de, lukas.pirl@hpi.de, robert.schmid@hpi.de,
richard.kahl@tu-dresden.de
- #3: Securing Railway Intrusion Detection Environments
simon.unger@uni-passau.de
- #4: Sicherheitsanalyse EULYNX
jonas.henschel@informatik.tu-chemnitz.de, martin.lehnert@th-wildau.de
- #5: IT-Sicherheitsanalyse von GSM-R
katja.assaf@hpi.de, lukas.ifflaender@htw-dresden.de

Summerschool

Camp Edition



- 28. bis 30. August 2024 in der Prignitz (Mittwoch nachmittag bis Freitag nachmittag)
- Organisation zusammen mit der DB Systel
- Summerschool besteht aus Workshops, Vorträgen, Exkursionen, Networking
- Teilnehmer sind Studierende und Firmenvertreter
- Anmeldung, Kosten etc. in den kommenden Wochen

zu überarbeiten

- Foliensatz kann bald auf der HPI-Webseite heruntergeladen werden:
osm.hpi.de/drss/2025/curriculum
- Aufgaben für alle Studierenden bis 29.4. 14 Uhr:
 - E-Mail an die Verantwortlichen für das jeweils gewählte Projekt
 - in die studentische Mailingliste eintragen (unser *und* euer Medium)
lists.hpi.uni-potsdam.de/listinfo/drss25-stud
 - Projektverantwortliche stimmen mit ihrer Gruppe den Auftakttermin ab
 - Wichtig: man kann auch ein Projekt an einer Uni machen, zu der man nicht gehört, aber es gelten die Prüfungsmodalitäten der Heimatuni

Ansprechpartner:innen (allgemein)



Birgit Milius (TUB)

birgit.milius@tu-berlin.de

Andreas Polze (HPI)

andreas.polze@hpi.de

Simon Unger (Uni Passau)

simon.unger@uni-passau.de

Matthias Werner (TUC)

mwerner@informatik.tu-chemnitz.de

Ulrich Maschek (TUD)

ulrich.maschek@tu-dresden.de

Martin Lehnert (TH Wildau)

martin.lehnert@th-wildau.de

alle: drss25-orga@hpi.de



hpi.de/drss

Digital Rail

Auftaktveranstaltung

23. April 2025